Davis Wright Tremaine LLP

1919 Pennsylvania Avenue NW
Suite 200
Washington, DC 20006-3402

Paul B. Hudson
202.973.4275 tel
202.973.4499 fax

paulhudson@dwt.com

February 26, 2010

VIA ELECTRONIC FILING

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

Re: EB Docket 06-36, Annual 47 C.F.R. § 64.2009(e) CPNI Certification

Annual § 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009
Date filed: February 26, 2010
Name of companies covered by this certification and Form 499 Filer IDs:

Armstrong Telephone Company – Maryland	**808080**
Armstrong Telephone Company – New York	**808083**
Armstrong Telephone Company – Pennsylvania	**808092**
Armstrong Telephone Company – West Virginia	**808095**
Armstrong Telephone Company – Northern Division	**808089**
Armstrong Telephone Company – North	**808086**

Name of signatory: **Jeffrey A. Ross**
Title of signatory: **President**

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's Rules, 47 C.F.R. § 64.2009(e), enclosed for filing in the above-referenced docket is the executed annual CPNI Compliance Certificate for Armstrong Telephone Company – Maryland; Armstrong Telephone Company – New York; Armstrong Telephone Company – Pennsylvania; Armstrong Telephone Company – West Virginia; Armstrong Telephone Company – Northern Division; Armstrong Telephone Company – North (together, "Company").

Attached to the certificate is a summary of Company's CPNI policies and procedures. Because some of the details included in that document could provide a roadmap for unauthorized persons to attempt to obtain CPNI, Company is filing only a redacted version with the Commission's electronic filing system. *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-115, Report and Order and Further Notice of

Proposed Rulemaking, FCC 07-22, n. 167 (rel. April 2, 2007) ("We recognize carrier concerns about providing a roadmap for pretexters with this annual filing, and thus we will allow carriers to submit their certifications confidentially with the Commission."). The redacted language was previously provided to the Enforcement Bureau in Company's prior-year filing in this docket, and has not changed.

Respectfully submitted,

Paul B. Hudson
Counsel for the Armstrong Telephone Companies

Enclosures

Annual 47 C.F.R. § 64.2009(e) CPNI Certification of Compliance

EB Docket 06-36

1. Annual § 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009
2. Date filed: February 26, 2010
3. Name of companies covered by this certification and Form 499 Filer IDs:

   Armstrong Telephone Company – Maryland, 808080
   Armstrong Telephone Company – New York, 808083
   Armstrong Telephone Company – Pennsylvania, 808092
   Armstrong Telephone Company – West Virginia, 808095
   Armstrong Telephone Company – Northern Division, 808089
   Armstrong Telephone Company – North, 808086

4. Name of signatory: Jeffrey A. Ross
5. Title of signatory: President
6. Certification:

I, Jeffrey A. Ross, certify that I am President of the companies named above (collectively "Company") and, acting as an agent of each of these companies, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Commission's rules governing use and disclosure of customer proprietary network information ("CPNI"), as governed by Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, and as set forth in Part 64, Subpart U of the of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not received any customer complaints in the past calendar year concerning unauthorized access to or release of CPNI. Company does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Company has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the Company at either state commissions, the court system or at the Commission. The Company has established procedures to report any breaches to the FBI and United States Secret Service, and it has emphasized in its employee training of the need for vigilance in identifying and reporting unusual activity in order to enable the Company to continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the

Commission are punishable under Title 18 of the U.S. Code and may subject the Company to enforcement actions.

Jeffrey A. Ross
President
Armstrong Telephone Company – Maryland
Armstrong Telephone Company – New York
Armstrong Telephone Company – Pennsylvania
Armstrong Telephone Company – West Virginia
Armstrong Telephone Company – Northern Division
Armstrong Telephone Company – North

Executed February 9, 2010

PUBLIC VERSION

Revised CPNI Compliance Policies of the Armstrong Telephone Companies

Revised Effective December 8, 2007

The following summary describes the policies of Armstrong Telephone Company–Maryland, Armstrong Telephone Company–New York, Armstrong Telephone Company–Pennsylvania, Armstrong Telephone Company–West Virginia, Armstrong Telephone Company–Northern Division, and Armstrong Telephone Company–North (collectively, including all employees, associates, and agents thereof, "Armstrong") that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*. Armstrong substantially revised and updated its policies and conducted new training prior to the effective date of the FCC's new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007).

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

Because the details of this policy could provide a roadmap for unauthorized persons to attempt to subvert these policies and attempt to obtain CPNI, copies of this policy and related training materials are classified as confidential and may be provided only to Armstrong employees or to parties approved by the CPNI Compliance Manager. [REDACTED]

Armstrong's policy, administered by its CPNI Compliance Manager, Terry Dickerhoof, Vice President of Customer Service Operations & Billing, establishes the following parameters regarding the use and disclosure of CPNI:

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

A. Use, Disclosure or Access to CPNI Without Customer Approval

Armstrong may use, disclose, or permit access to CPNI without customer approval in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Armstrong, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to market services within the category or categories of services to which the customer already subscribes, including, for local exchange customers, to market services formerly known as adjunct-to-basic services (such as, but not limited to, speed dialing, computer-provided directory assistance, call

monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features), and, for local exchange or interexchange customers, to market CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store-and-forward, and protocol conversion services; and to provide inside wiring installation, maintenance, or repair services; or as required by law.

B. Customer Approval of Use, Disclosure and Access to CPNI

Armstrong may use, disclose, or permit access to CPNI as expressly authorized by the customer.

Armstrong may use, or disclose or permit access, by its agents and affiliates that provide communications-related services, to a customer's individually identifiable CPNI to market to that customer any communications-related service offerings that are not within a category of service to which the customer already subscribes, but only with prior "opt-out" approval from the customer in accordance with the following procedures set forth in this section I.B.

A customer is deemed to have provided "opt-out" consent to such use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within 33 days following Armstrong's mailing of a comprehensible, non-misleading individual written notification that provides sufficient information to enable the customer to make an informed decision as to whether to permit Armstrong to use, disclose, or permit access to, the customer's CPNI, and that includes all of the following elements:

- prior to any solicitation for customer approval, explains that the customer has a right to restrict use of, disclosure of, and access to their CPNI, and that Armstrong has a duty, under federal law, to protect the confidentiality of CPNI;
- specifies the types of information that constitutes CPNI and the specific entities that will receive the CPNI;
- describes the purposes for which CPNI will be used;
- informs the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time;
- advises the customer of the precise steps the customer must take in order to grant or deny access to CPNI;
- states clearly that a denial of approval will not affect the provision of any services to which the customer subscribes;
- is clearly legible, in sufficiently large type, and placed in an area so as to be readily apparent to a customer;
- does not include any statement encouraging a customer to freeze third-party access to CPNI;

- states that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial, and that if the customer has opted-out previously, no action is needed to maintain their opt-out election; and

- states that customer's approval may be assumed by Armstrong if customer does not object to such use within 33 days of the mailing of the notice.

Armstrong makes available to every customer a method to opt-out that is of no additional cost to the customer and is available 24 hours a day, seven days a week.

Armstrong does not seek customer opt-out approval at any time that is not proximate to its provision of the above notification.

At this time, Armstrong does not provide notifications in languages other than English. If any part of a notification is translated into another language, all portions would be translated into that language.

Approval or disapproval to use, disclose, or permit access to a customer's CPNI shall remain in effect until the customer revokes or limits such approval or disapproval. However, to rely on a customer's prior out-out approval, Armstrong must provide a new notification to such customer every two years.

Armstrong may also use, disclose, or permit access to CPNI to provide inbound marketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of Armstrong's use to provide such service. In requesting such approval, the Armstrong representative must explain that the customer has a right, and that Armstrong has a duty, under federal law, to protect the confidentiality of CPNI; specify the types of CPNI that would be used for the call and the purposes for which it would be used; inform the customer of his or her right to decline such use and that such denial will not affect the provision of any services to which the customer subscribes; and will not attempt to encourage a customer to freeze third-party access to CPNI.

Armstrong shall provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly to such a degree that consumers' inability to opt-out is more than an anomaly. Such notice shall be in the form of a letter, and shall include Armstrong's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information. Such notice must be submitted even if Armstrong offers other methods by which consumers may opt-out.

All uses of CPNI for outbound marketing and any request for customer approval for such use must be pre-approved by a marketing supervisor or the CPNI Compliance Manager. In the event that the proposed use requires customer's prior approval, such as use in outbound marketing of communications-related services that are not within a category of service to which the customer

already subscribes, this supervisory review process includes a review of the status of each customer's CPNI approval to assure that a customer's CPNI approval status can be clearly established prior to the use of CPNI.

All use or disclosure of CPNI for marketing and all requests for customer approval for such use must be pre-approved through Armstrong's supervisory review process that involves a supervisor designated by the senior employee responsible for marketing and the CPNI Compliance Manager.

C. Other Restrictions on Use of CPNI

Armstrong does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Armstrong receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Armstrong will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Armstrong's existing policies that would strengthen protection of CPNI, they should report such information immediately to Armstrong's CPNI Compliance Manager so that Armstrong may evaluate whether existing policies should be supplemented or changed.

A. Establishment of CPNI Passwords and Security Questions

Armstrong enables customers to establish a CPNI Password for each telephone account. [REDACTED]

B. Inbound Calls to Armstrong Requesting CPNI

Call Detail Information (CDI) includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Armstrong will not disclose CDI to an inbound caller unless the caller is authenticated as the customer by correctly providing the CPNI Password or the answer to the Security Question associated with the account.

Armstrong may also send a copy of a bill or requested CDI to an address of record for the account, but only if such address has been on file with Armstrong for at least 30 days. In the event that a customer has changed their address within the prior 30 days, or for appropriate

circumstances, Armstrong may discuss CDI with a customer on the phone, but only in a call initiated by Armstrong and placed to the customer's telephone number of record.

If an inbound caller is able to provide to the CSR the telephone number called, the time of the call, and, if applicable, the amount charged for the call, exactly as that information appears in Armstrong's records, then the CSR is permitted to discuss customer service pertaining to that call and that call only. [REDACTED]

For CPNI other than CDI, CSRs require an inbound caller to authenticate their identity through [REDACTED].

C. Online Accounts

At this time, Armstrong does not offer online accounts that provide access to any CPNI. If Armstrong offers such access in the future, it will revise these policies to comply with the FCC's requirements for password protection of such accounts.

D. In-Person Disclosure of CPNI at Armstrong Offices

Armstrong may disclose a customer's CPNI to an authorized person visiting an Armstrong office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

E. Notice of Account Changes

Armstrong will send a notification to a customer's address of record immediately whenever a password, CPNI Password, Security Question, online account, or address of record is created or changed, except for such events that occur during the period when the customer initiates service. When such a change is made to an address of record, the notice will be sent only to a pre-existing address of record. The notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Armstrong if they have any questions regarding the change.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Armstrong employee that becomes aware of any breaches, suspected breaches or attempted breaches of CPNI must report such information immediately to the Armstrong CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Armstrong's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law

enforcement promptly. Therefore, although employees who violate Armstrong's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If an Armstrong employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Armstrong's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Armstrong's CPNI Compliance Manager will determine whether it is appropriate to update Armstrong's CPNI policies or training materials in light of any new information; the FCC's rules require Armstrong on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. Armstrong's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions.

Armstrong will not under any circumstances notify customers or disclose a breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI except as provided below (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure.

If Armstrong receives no response from law enforcement after the seventh (7^{th}) full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Armstrong will delay notification to customers or the public upon request of the FBI or USSS. If the CPNI Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Armstrong still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The CPNI Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Armstrong maintains a record, for a period of at least one year, of: those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI; of supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI; its sales and marketing campaigns that use its customers' CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services offered as a part of the campaign; and records associated with customers' "opt-out" approval or non-approval to use CPNI, and of notification to customers prior to any solicitation for customer approval of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

Armstrong maintains a record of all customer complaints related to their handling of CPNI, and records of Armstrong's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Armstrong considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Armstrong will have an authorized corporate officer of each of the companies identified above, as an agent of such companies, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Armstrong has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Armstrong's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

[REDACTED] All employees with such access to CPNI receive a copy of Armstrong's CPNI policies and are informed that (i) Armstrong takes seriously the protection of its customers' CPNI, and any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Armstrong requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel. [REDACTED]